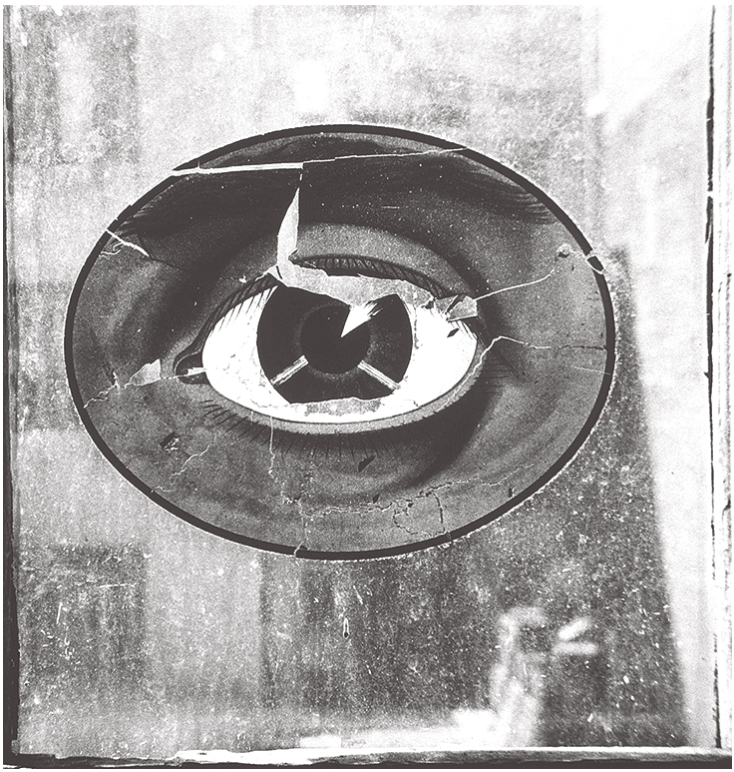
Matthieu Amiech

# Surveillance « intelligente »

## *vers le règne de l'arbitraire techno-bureaucratique ?*



2024

**Matthieu Amiech** est un des animateurs des éditions La Lenteur.

Il a participé à la rédaction de l'ouvrage du groupe MARCUSE, *La Liberté dans le coma. Essai sur l'identification électronique et les motifs de s'y opposer* [2012], La Lenteur, 2019.

Il est l'auteur de

— *L'Industrie du complotisme. Réseaux sociaux, mensonges d'État et destruction du vivant*, La Lenteur, 2023.

— *Peut-on s'opposer à l'informatisation de nos vies ?*, La Lenteur, 2024.

Il est également membre du groupe *Écran Total, résistance à la gestion et l'informatisation de nos vies* depuis 2013.

Éditions La Lenteur,
Le Batz,
81 140 St Michel de Vax

Illustration de couverture :
Nathan Lerner, *Eye on Window*, 1943.

# Surveillance « intelligente »

## *vers le règne de l'arbitraire techno-bureaucratique ?*

Au début de 2023, en marge d'un dossier sur les dangers des ondes électromagnétiques pour la santé, le premier numéro du journal d'investigation *La Brèche* proposait une série de petits articles et entretiens sur les retombées du mode de vie numérique en matière de liberté et de surveillance. En deux pages, au moins cinq facettes de ces évolutions étaient évoquées : « Les preuves d'un avortement illégal fournies à la police [du Nebraska] par… Facebook » ; « Lopmi, une loi pour "une vision fantasmée des policiers connectés" » ; « Appariement algorithmique : "des dispositifs qui soulèvent des questions politiques" » ; « Des outils de Google mis à la disposition d'Israël [pour surveiller la population palestinienne] » ; « Bracelet connecté [pour les collégiens de la Sarthe] : un progrès à grands pas ».

La banalisation des technologies d'intelligence artificielle à des fins de surveillance provoque ainsi quelques remous dans la société française, à défaut du débat approfondi qui serait à la hauteur des enjeux. Les alarmes tirées par différents acteurs, depuis le début des années 2000, sur le déclin rapide des libertés publiques du fait de certaines innovations numériques semblent actuellement se concrétiser autour de différents dispositifs : en premier lieu, le développement de la vidéosurveillance algorithmique et le recours possible à des logiciels de reconnaissance faciale ; mais aussi les algorithmes de notation des citoyens, qui, combinés aux avancées de l'identité numérique, font planer le spectre d'un système de crédit social général, dans des pays pourtant marqués par la tradition du libéralisme politique.

Pour l'association *La Quadrature du Net*, qui mène un travail important d'enquête, de critique publique et de recours juridiques à ces sujets, « la reconnaissance faciale change le visage du monde » et est porteuse d'un « changement anthropologique » [1]. Bien que le système de vidéosurveillance

[1] Voir la brochure de l'association : *Le vrai visage de la reconnaissance faciale*, p. 17.

algorithmique déployé par la municipalité de Nîmes ne puisse pour l'instant recourir à la reconnaissance faciale, le vice-président de l'antenne nîmoise de la Ligue des Droits de l'homme, Jean Launay, parle d'une « surveillance de masse » et s'inquiète : « le droit à la vie privée passe par l'existence d'une sphère privée. Et force est de constater que cette sphère, à Nîmes, se réduit comme peau de chagrin. » Quant à Thomas Dautieu, directeur de l'accompagnement juridique (sic) de la Cnil, il déclare gravement :

> « Les systèmes deviennent de plus en plus performants, avec des caméras numériques capables de faire du 360 degrés et de zoomer. Et il y a un nouveau phénomène ; certaines d'entre elles sont augmentées, c'est à dire qu'elles ne se contentent pas de filmer, elles peuvent analyser. […] Ces systèmes sont susceptibles de modifier votre comportement dans l'espace public. Si l'individu sait qu'il va déclencher une alerte s'il se met à courir, peut-être qu'il ne va pas courir. Et cela doit tous nous interpeller. » [2]

Mon article vise à nous demander ce qu'il y a précisément de nouveau dans ces nouveautés, et où se situent les éventuels basculements. Je resituerai les évolutions les plus récentes dans le processus d'informatisation des sociétés humaines des trente dernières années, qui détermine largement, au-delà de telle ou telle application particulière, le recul considérable des possibilités d'anonymat et de vie privée dans ces sociétés. Je me pencherai ensuite sur les conséquences des étapes actuelles du déferlement technologique en matière de libertés civiles, en mettant en avant la montée de l'arbitraire bureaucratique à mesure que s'étend le champ d'application de la soi-disant intelligence artificielle.

## La surveillance, revers inévitable du mode de vie connecté

Dans un ouvrage collectif auquel j'ai participé, *La Liberté dans le coma*, publié pour la première fois en 2012, le groupe MARCUSE affirmait le caractère inévitable de la surveillance technologique, dans un monde de plus en plus informatisé et connecté. Cela peut bien sûr paraître un truisme, mais c'est un truisme rarement perçu et si peu ressenti par la plupart de nos

[2] Ces propos, comme ceux de Jean Launay, sont tirés de l'article d'Antoine Albertini et Agathe Beaudoin, « Pourquoi les "hyperviseurs" urbains suscitent engouement et craintes », *Le Monde*, 9 janvier 2024.

contemporains : les capacités de surveillance des individus par l'État et les entreprises ne peuvent avoir pris une telle ampleur que parce qu'une grande partie de la population utilise en permanence des artéfacts électroniques connectés au réseau Internet. Et ce qui était vrai au début des années 2010 l'est *a fortiori* au milieu de la décennie 2020 : sans un usage aussi intensif (en fait, *toujours plus intensif*) de ces appareils et de leurs applications foisonnantes, une partie importante de cette surveillance ne pourrait pas exister, en tous cas pas sous la même forme et au même prix.

Le point de départ de notre réflexion était une interrogation sur le recul des libertés civiles provoqué par des technologies comme la biométrie ou les puces RFID, dont le déploiement dans la vie courante a commencé environ en 2005. Mais à partir de nos questions sur l'ampleur exacte de ce recul, nous arrivions à la critique d'un mode de vie, car il s'avérait que les progrès de la surveillance n'étaient jamais dissociables des progrès de l'informatique en général et de ses autres usages – organiser le travail et la production, maîtriser la consommation, recenser les populations et mettre en place des systèmes assurantiels privés ou publics, jouer, s'informer, sophistiquer les armes de guerre… Après avoir montré dans le premier chapitre que le développement de l'informatique depuis 1880 était largement tributaire des impératifs de gestion de masse traversant les administrations et les industries modernes, nous aboutissions au début du deuxième chapitre à cette mise au point :

> « Le problème de la surveillance est généralement présenté comme une incidence évitable – au prix d'un minimum de garde-fous légaux – d'un mode de production et d'un type d'existence qui seraient en eux-mêmes porteurs de liberté. Or, considérer la surveillance comme un aspect négatif mais contingent des technologies de l'information et de la communication est absurde. Il n'est pas possible, par exemple, d'opposer les prétendus avantages des cartes RFID aux possibilités de contrôle à distance qu'elles recèlent. La technologie RFID repose sur la transmission automatisée de données d'une machine à une autre (de la puce au lecteur, du lecteur à l'ordinateur, etc.), la possibilité d'un contrôle instantané en découle donc directement. C'est le principe même de cette technique que de relever systématiquement les traces de contacts électroniques.
>
> Plus globalement, à partir du moment où l'ensemble de nos activités sont informatisées, il y a beaucoup plus d'informations sur nous et elles ne peuvent jamais dans leur totalité être effacées, rendues anonymes ou inutilisables. De même qu'il est impossible de bâtir une maison en amiante où personne ne

> serait jamais en contact avec de l'amiante, de même il est illusoire de penser que l'informatisation de la vie sociale pourrait ne pas générer des torrents d'informations sur toutes choses, à toutes fins utiles. Google est essentiellement une entreprise de surveillance puisque sa raison sociale est d'accumuler des données sur tout et sur tous. Les compagnies de téléphonie mobile sont pratiquement des services auxiliaires de la police, chargés de la géolocalisation des individus tenus en laisse par leur portable.
>
> […] les phénomènes de fichage et de surveillance ne sont que le corollaire d'une organisation de l'existence qui a privé les foyers et les communautés de base de toute prérogative directe sur leurs moyens de subsistance. Nous savons que les organisations impersonnelles, qui pourvoient non seulement à nos besoins élémentaires, mais aussi à tous ceux que nous les avons laissé inventer, prospèrent sur le mensonge, l'expropriation, le saccage et souvent le crime. Mais nous leur devons notre vie ici-bas. Ce qui rend obsolètes les concepts politiques élémentaires du XIX[e] siècle, "liberté de conscience", "résistance à l'oppression", "protection de la vie privée et respect du domicile", ce ne sont pas simplement les innombrables dossiers dont ces organisations disposent sur nous. C'est le gigantisme industriel lui-même, tel qu'il s'est déployé au cours des deux siècles écoulés à l'ombre des libertés "bourgeoises". » [3]

À contre-courant des nombreux discours des années 2000 sur les gains d'autonomie permis par le numérique (dans le travail, en politique, dans la vie personnelle), l'informatisation nous paraissait donc un nouveau pas des populations industrialisées vers l'hétéronomie. Nous retrouvions la notion de « vie administrée » qu'avaient mis en avant les auteurs de l'École de Francfort (Adorno, Horkheimer, Marcuse…) pour décrire les évolutions des années 1950-60 : la société numérique comme un stade supérieur de dépendance matérielle et mentale des humains au capitalisme et aux grandes organisations, en comparaison de la première « société de consommation ». C'est qu'avant même le stade actuel de l'intelligence artificielle, l'informatisation était déjà un formidable levier de mise en chiffres des comportements humains. Le recueil de données tous azimuts et les calculs réalisés à partir d'elles permettent d'établir des déterminismes – les établir, c'est-à-dire à la fois les déceler et les entretenir, ou les amplifier.

Au final, il ne s'agissait donc plus seulement de savoir si la biométrie ou les puces ruinaient les vieilles « garanties » (toujours relatives) contre

[3] Groupe MARCUSE, *La Liberté dans le coma. Essai sur l'identification électronique et les motifs de s'y opposer*, Vaour, La Lenteur, 2019, p. 125-126, puis 155-156.

l'arbitraire étatique et policier. Il s'agissait plutôt de se demander si ce n'est pas le recul du désir et des possibilités concrètes de vivre librement qui provoque le déclin des libertés civiles, à tout le moins qui explique l'indifférence dans laquelle elles sont mises à mal. Tout en appelant à la résistance culturelle et à la désobéissance civile face à l'injonction numérique, nous faisions l'hypothèse d'une dialectique négative entre progrès de la puissance algorithmique et déclin de la liberté : le risque est que plus la société dispose de statistiques pour enfermer les gens dans des déterminismes, plus le désir d'être libre recule chez les individus.

Les différents éléments de ce diagnostic me semblent (malheureusement) largement confirmés par ce qui s'est produit depuis 2012. En premier lieu, les progrès de la surveillance des populations reposent largement sur les usages plus ou moins addictifs du numérique adoptés par une bonne partie d'entre elles. Ainsi, pourquoi est-il plus aisé aujourd'hui qu'il y a quinze ans de géolocaliser des individus, d'installer sur leur smartphone un logiciel-espion, de mettre en place à grande échelle une application de Pass vaccinal ou de Portefeuille d'identité numérique ? Parce que la majorité des gens ont un smartphone, et qu'ils l'utilisent pour un très grand nombre d'actes de la vie quotidienne. Pour beaucoup, il est proprement impensable de s'en passer, de ne pas s'en servir dans les transports, de ne pas payer avec (« sans contact »), de ne pas l'utiliser pour s'orienter, chercher une information ou envoyer des messages à tout moment. Et au-delà d'un phénomène de norme sociale, c'est toute l'organisation sociale qui chaque jour un peu plus escompte que chacun dispose de cet appareil et pousse à s'en munir. Les usages se multiplient sans fin, et presque tous offrent de nouvelles informations sur la vie des personnes, que la puissance de calcul des ordinateurs permet de mieux profiler, intégrer dans des systèmes automatisés de promotion commerciale et de paiement, ou signaler comme « anomalies ».

L'évidence du smartphone s'accompagne de l'évidence du fait de photographier et filmer à tout bout de champ ce qui arrive autour de soi ; puis, souvent, de mettre en ligne. Cette évidence de la vidéo, combinée à la multiplication du recours aux caméras par les commerçants et même les particuliers (sans parler de toutes celles posées par les institutions), est un élément important de la surveillance qui peut s'exercer. Elle contribue à une atmosphère que de nombreuses personnes vivent comme normale et non contrariante, mais qui à coup sûr ne favorise pas l'expression excentrique, non

conformiste, subversive. Cette atmosphère est renforcée par le fonctionnement ordinaire des réseaux sociaux, même quand il ne s'agit que d'expression écrite et non d'images. Ces réseaux fournissent des quantités faramineuses d'informations aussi bien aux départements de marketing qu'aux services de renseignement et de police [4].

Et même si l'on élude un instant cette dimension de surveillance, qu'est-ce qui nourrit, entraîne, consolide, une intelligence artificielle ? Ce sont les données recueillies par des machines et transmises par Internet. Les intelligences artificielles sont entraînées grâce aux millions et milliards de traces laissées par les internautes sur des sites Internet – de jour comme nuit, à la maison ou en déplacement ; grâce aux flashes des QR-codes disséminés partout dans l'espace public ; grâce aux données des « services publics » qui suppriment leurs guichets et obligent leurs usagers à livrer des tombereaux d'informations personnelles en échange de leur prestation ; grâce encore aux ordinateurs de bord des voitures semi-automatiques, qui enregistrent des quantités prodigieuses de chiffres sur la conduite du véhicule et d'images sur son passage.

On voit bien avec ces différents exemples que la frontière est désormais floue et ténue entre les formes de surveillance consenties par les habitants de la *smart city* et celles qu'ils subissent à leur insu. Dans son rapport de 2021 sur technologies biométriques et droits fondamentaux, la Défenseure des droits tient à distinguer les technologies *actives* (où l'individu fournit volontairement des informations, par exemple en enregistrant de son plein gré un de ses caractères physiques pour permettre son authentification par la suite), des technologies *passives* (où les informations biométriques sont détectées à l'insu de la personne). Son inquiétude pour le devenir des droits fondamentaux est donc focalisée sur la vidéosurveillance dans les rues, les transports publics, les immeubles, par drones, notamment quand les caméras utilisées sont dotées de logiciels capables d'identifier des personnes dont le visage figure au préalable dans des bases de données [5].

Mais que penser des données recueillies sur la vie privée des foyers par les compteurs Linky ? Le *Big data* et la surveillance qui en découlent ont-elles

[4] J'ai déjà évoqué dans l'introduction « Les preuves d'un avortement illégal fournies à la police par… Facebook », *La Brèche* n°1, janvier-février 2023.

[5] Claire Hédon, *Rapport – Technologies biométriques : l'impératif respect des droits fondamentaux*, 19 juillet 2021, p. 12.

été obtenues de gré ou de force ? Tantôt l'un, quand des personnes ont accepté de nouveaux compteurs avec enthousiasme ou indifférence, tantôt l'autre, quand certaines ne l'ont laissé entrer chez eux que suite à des menaces de procès, d'amende, ou même par des procédés à la limite de l'intimidation physique [6]. Que penser des données recueillies par « Mon espace santé » ? Cet espace numérique personnel a été ouvert d'office par l'Assurance maladie à des millions de personnes qui ne l'ont pas choisi, seule une minorité étant informée que son attribution pouvait être refusée. Et le Pass sanitaire de 2021 ? Choix libre et éclairé (« tous vaccinés, tous protégés »), ou dispositif électronique de contrainte à la vaccination sous peine de privations difficilement supportables ?

En Russie, les clichés de reconnaissance faciale grâce auxquels les citoyens peuvent payer dans les transports en commun et les supermarchés permettent aussi de rattraper et arrêter ceux qui veulent échapper à la mobilisation militaire pour « l'opération spéciale » en Ukraine [7]. Et en Occident, les entreprise Clearview (US) et PimEyes (Pologne) revendent aux forces de l'ordre, ou à des particuliers, des fichiers biométriques constitués à partir de millions de photographies laissées sur Internet, parfois mises en ligne par les intéressés eux-mêmes [8]. Technologie active ou technologie passive ? Surveillance autogérée ou société de contrainte ? Bien malin qui peut le dire catégoriquement.

Nous sommes face à un mode de vie qui nous enveloppe de tous côtés. Dans des conditions données, à bien des égards de plus en plus contraignantes, les individus acceptent de disposer de moins en moins d'autonomie dans tous les domaines de leur existence : au volant de leur voiture, ils s'en remettent à de nombreux automatismes ; chez eux, ils se font servir par un assistant vocal ; en matière de santé, certains utilisent des applications comptant leurs battements de cœur et leurs pas… Il en découle un élargissement constant des possibilités de surveillance par des acteurs publics et privés, un déclin continu des possibilités d'anonymat dans la société de

[6] Voir la revue de presse de Stéphane Lhomme, « Des actes inadmissibles commis contre la population par les installateurs de compteurs Linky », <http://refus.linky.gazpar.free.fr/>

[7] Voir Margaux Vulliet, « La Russie utilise la reconnaissance faciale pour traquer conscrits et opposants », <www.bfmtv.com/>, 2 novembre 2022.

[8] Voir Florian Reynaud, « Reconnaissance faciale : une enquête demandée à la Cnil sur les pratiques de Clerview », *Le Monde*, 27 mai 2021 ; et « PimEyes : A Polish company is abolishing our anonymity », <netzpolitik.org>, juillet 2020.

masse, et une indifférence profonde à ce déclin qui semble inévitable au plus grand nombre.

Cette indifférence est particulièrement frappante en ce qui concerne les impacts de l'usage de l'intelligence artificielle sur les libertés publiques. Mais peut-on se soucier sérieusement des possibilités d'identification des personnes par reconnaissance faciale, ou des discriminations à l'embauche sur la base des émotions perçues par des algorithmes, si l'on n'a pas de réticence à remettre tant de prérogatives humaines aux mains des machines ? Dans ce qui fait figure de débat médiatique sur les fameux « dangers de l'I.A », c'est toujours la fascination qui domine, la soumission à un fait accompli technologique devant lequel les principes éthiques et politiques sont pliés avant même d'avoir été évoqués. Des journalistes du *Point*, toujours au summum de l'indignation devant le piétinement des libertés civiles en Iran ou en Russie, ne sont plus attachés à aucun principe lorsqu'ils parlent d'une technologie venue de la Silicon Valley, dont ils admettent pourtant qu'elle vise à rien moins que « contrôler nos cerveaux » :

> « En ce mois de novembre 2023, ChatGPT n'a pas encore soufflé sa première bougie qu'on sait déjà que rien ne sera plus comme avant. Dans les livres d'histoire, c''est certain, il y aura bien un avant et un après la mise à disposition à plus de 100 millions d'utilisateurs de ce robot conversationnel qui sait tout faire ou presque : vous conseiller en une poignée de secondes sur une recette de cuisine en fonction des aliments qui traînent dans votre frigo, créer un site Web à partir d'un croquis ou vous renseigner, à partir d'une simple photo, sur la pièce à changer dans le moteur de votre voiture en panne.
>
> Sam Altman, son inventeur, tout comme celui du logiciel d'images Dall-E, se plaît à rappeler qu'il est né un 22 avril comme Robert Oppenheimer, le père de la bombe atomique… Comme si ces deux scientifiques avaient chacun à sa façon changé la face du monde. L'avènement de l'intelligence artificielle a commencé à révolutionner le XXI[e] siècle et l'on entrevoit seulement la partie émergée de l'iceberg, tant les perspectives sont infinies : prédiction des maladies, lutte contre le changement climatique, accélération de la productivité, etc. » [9]

[9] Guillaume Grallet, Héloïse Pons, « Intelligence artificielle. La bataille pour contrôler nos cerveaux », *Le Point*, 30 novembre 2023.

## Des technologies qui contournent les garde-fous légaux, malgré leur efficacité douteuse

Quels seuils sont franchis par les technologies dites d'intelligence artificielle en matière de (recul des) libertés publiques ? La Défenseure des droits souligne un risque d'atteinte grave au respect de la vie privée par les systèmes biométriques, en premier lieu de reconnaissance faciale. L'identification directe de personnes dans l'espace public (et ou dans une foule), parce que leur visage figurait au préalable dans une base de données, marque effectivement un seuil supplémentaire dans la difficulté à conserver l'anonymat dans la société numérique. La Défenseure évoque également, à propos de la vidéosurveillance algorithmique en général, un possible effet dissuasif dans l'exercice de certains droits politiques fondamentaux comme la liberté d'expression, le droit d'aller et venir, de former une assemblée ou une association, voire d'accéder à des services de base comme les soins en cas d'affection ou de blessure graves.

Une illustration directe de ces mises en garde est fournie par les amendes infligées à trente manifestants de Millau, lors de défilés dénonçant la responsabilité des autorités dans l'affaiblissement du système de santé publique, à l'issue du confinement de mars-mai 2020. Ces personnes ont reçu leur amende par courrier, sans avoir été verbalisées au préalable, ni lors de la manifestation non déclarée du 12 mai, ni lors de celle (déclarée) du 22 mai. Les autorités ont d'un côté contesté que les sanctions aient été prises sur la base d'images de vidéosurveillance (il y avait alors 48 caméras de surveillance dans la ville), en arguant que les policiers et agents du renseignement présents connaissaient déjà les incriminés ; et d'un autre côté, ils ont validé cette thèse défendue par les accusés, en reconnaissant que les images avaient été utilisées pour identifier de manière formelle des personnes déjà fichées. On est donc bien face à l'exemple d'une police qui utilise les technologies de pointe pour dissuader la population d'exprimer ses opinions et de contester le pouvoir en place [10].

[10] Il n'est pas clair si la reconnaissance faciale en tant que telle a été utilisée pour ces identifications à distance ; mais même en admettant que ces identifications-là aient été faites « à l'œil », sur les écrans (pour compléter ce qui avait été pré-établi d*e visu* ?), il ne fait pas de doute

Au-delà de ces constats en tant que tels édifiants, un certain nombre de garde-fous contre la surveillance des citoyens tombent aussi parce que certaines technologies de fichage et d'identification sont mises en œuvre par des entreprises privées qui ne sont pas soumises aux mêmes restrictions que des administrations publiques. Aussi bien Kate Crawford qu'Asma Mhalla font le constat d'un brouillage de la frontière entre secteur public et secteur privé en matière de surveillance, et s'accordent pour dire que cela a de lourdes conséquences sur le respect des lois existantes [11]. Ce brouillage a commencé quand les géants américains du numérique ont collaboré avec la NSA (National Security Agency), dans les années 2000-2010, pour lui permettre de recueillir des données sur tous les échanges téléphoniques et électroniques à l'échelle du monde ; il s'est prolongé à partir de 2016 avec la demande explicite du Pentagone aux entreprises de la Silicon Valley de mettre leurs compétences en matière d'intelligence artificielle au service de l'armée américaine, pour lui permettre de se doter d'un nouvel avantage militaire sur ses rivales russes et chinoises (*Third Offset Strategy* et Projet Maven [12]).

Mais le brouillage est bien plus général et diffus que cela. Palantir, l'entreprise de Peter Thiel et Alex Carp, n'a pas seulement travaillé pour la NSA, le FBI et la CIA (qui a participé à son financement, à travers une société de capital-risque, In-Q-Tel). Elle est aussi devenue un fournisseur de surveillance externalisée pour l'ICE (Immigration and Customs Enforcement), dont elle a conçu les bases de données et les logiciels ; pour des services de police municipaux, qu'elle aide à organiser sa lutte contre la délinquance ; et pour le Département de la santé et des services sociaux, qu'elle aide à détecter les fraudes à Medicare (l'assurance-maladie). Des

---

que vidéosurveillance algorithmique et reconnaissance faciale pourront, *a fortiori*, être utilisées dans le même dessein de sanction-intimidation, une fois banalisées. Sur les faits, voir Pierre-Louis Caron, « Des manifestants ont-ils été verbalisés sur la seule base d'images de vidéosurveillance ? », <www.francetvinfo.fr>, 23 juin 2021.

[11] Kate Crawford, *Contre-atlas de l'intelligence artificielle. Les coûts politique, sociaux et environnementaux de l'IA* [2021], Zulma éditions, 2023 (voir le ch. 6, « L'État ») ; et Asma Mhalla, *Technopolitique. Comment la technologie fait de nous des soldats,* Seuil, 2024 (voir le ch. 10, « La doctrine de l'information totale »).

[12] La *Third Offset Strategy* a été lancée par le secrétaire à la Défense d'Obama en 2015-2016, Ash Carter, pour redonner l'avantage militaire à l'armée américaine grâce à un nouveau saut technologique ; il en découla en 2017 la création d'une « équipe interfonctionnelle de guerre algorithmique », chargée notamment d'organiser la collaboration entre le Pentagone et les géants du numérique de la Silicon Valley. Voir Kate Crawford, *op. cit*., p. 216 à 223.

technologies créées pour dénicher, n'importe où sur la planète, des terroristes susceptibles de reproduire une attaque comme celle du 11 septembre 2001, sont désormais utilisées pour tracer et évaluer des Américains ordinaires dans leur quartier, dans les supermarchés, à la sortie des écoles.

> « [Pour permettre l'appréhension de sans papiers dans les écoles et sur les lieux de travail,] Palantir a créé une appli téléphonique appelée FALCON, qui fonctionne comme un vaste filet pour rassembler des données provenant de multiples bases de données publiques et policières où figurent les antécédents familiaux, les informations professionnelles et le parcours scolaire. En 2018, des agents de l'ICE ont utilisé FALCON pour guider leurs raids dans une centaine de magasins 7-Eleven à travers les États-Unis. […]
>
> Dans une application innocemment intitulée "Systèmes de bases de données et interfaces utilisateurs pour l'analyse et l'identification d'image dynamique et interactive", Palantir se vante de pouvoir photographier les gens lors de très brèves rencontres et, qu'ils soient suspects ou non, de comparer leur image dans toutes les bases de données disponibles. En substance, le système utilise la reconnaissance faciale et le traitement des données en arrière-plan pour créer un cadre sur lequel fonder n'importe quelle arrestation ou expulsion. » [13]

Autre exemple : l'entreprise Vigilant Solutions, qui a installé des caméras de reconnaissance automatique des plaques d'immatriculation sur des voitures, des réverbères, des parkings, des immeubles, dans des dizaines de villes américaines. Elle vend l'accès à ses bases de données à la police, aux détectives privés, aux banques, aux compagnies d'assurance, etc. Elle met ainsi en œuvre des outils de surveillance qui pourraient nécessiter un contrôle judiciaire s'ils étaient utilisés directement par des agences gouvernementales. En tant qu'acteur privé vendant ses prestations sur le marché, elle est affranchie des limites constitutionnelles du respect de la vie privée et permet aux dites agences de s'en affranchir. Par exemple, l'ICE est contrainte de limiter sa collecte de données sur les personnes près de « lieux sensibles », comme les écoles, les églises et les manifestations. Mais en achetant l'accès aux systèmes de Vigilant Solutions, elle récupère *de facto* ces informations sans violer la loi.

On retrouve là un des caractéristiques du système technicien tel que le définit et l'analyse Jacques Ellul : il se déploie en écartant (en écrasant…) les

[13] Kate Crawford, *op. cit.*, p. 227.

barrières juridiques que l'on pense initialement capables de le réfréner [14]. La technologie s'impose en créant sa propre normalité, un fait accompli face auquel manque une volonté politique claire, qui nécessiterait à la fois d'adapter rapidement (autant de fois que nécessaire) les lois pour en préserver les principes fondamentaux, et de brider l'innovation ou ses usages. Ce qui est particulièrement inenvisageable aux États-Unis, comme le souligne André Vitalis [15].

Pourtant, les technologies basées sur l'intelligence artificielle sont d'une efficacité fort incertaine. Celles dont le fonctionnement pose le plus de problèmes et de doutes, d'un point de vue scientifique et technique, sont les technologies dites d'évaluation, qui visent notamment à identifier des émotions, des traits de personnalité ou des intentions à partir de données biométriques (voix, mouvements du visage…). Or, les fondements scientifiques de ces technologies sont considérés comme très fragiles par de nombreux chercheurs.

> « La littérature scientifique existante démontre que ces technologies sont très biaisées et commettent de nombreuses erreurs. Pour les chercheurs, détecter les émotions d'une personne avec précision et fiabilité dépendrait d'un contexte allant au-delà du visage et du corps. Des échantillons de voix ou onomatopées comme des mouvements du visage ne suffiraient pas à caractériser des émotions humaines et encore moins à évaluer avec rigueur les futures performances d'un candidat à l'embauche. » [16]

Plus largement, la Défenseure des droits souligne que toute technologie biométrique est probabiliste et repose sur l'emploi d'algorithmes présentant un certain taux de faux-positifs et de faux-négatifs. Ainsi, quand un dispositif biométrique est déployé pour authentifier ou identifier des centaines de milliers d'individus, même un faible taux de faux-positifs ou faux-négatifs implique que des dizaines ou centaines d'entre eux subissent les erreurs de ce dispositif. Les technologies de reconnaissance faciale « en temps réel » destinées à identifier des personnes recherchées s'avèrent ainsi très faillibles : en cause, les défauts de qualité de la source des images

[14] Jacques Ellul, *Le Système technicien* [1977], Paris, Le Cherche-midi, 2004.

[15] Voir, d'André Vitalis, « Surveillance numérique, sécurité et démocratie », document de travail de 2020, p. 2 et 3. Vitalis est co-auteur avec Armand Mattelart, du livre *Le Profilage des populations*, Paris, La Découverte, 2014.

[16] Claire Hédon, *Rapport – Technologies biométriques, op. cit.*, p. 6.

collectées et comparées, mais aussi les biais discriminatoires des données d'entraînement des algorithmes. Avec pour conséquences :

> « Aux États-Unis, trois hommes noirs ont déjà été emprisonnés injustement suite aux erreurs de systèmes de reconnaissance faciale. Au Royaume-Uni, une étude dédiée à l'utilisation de reconnaissance faciale aux fins d'identification par les services de police de Londres a déterminé que sur 22 individus interpellés sur la base d'une concordance établie par ordinateur et jugée crédible par un opérateur humain, quatorze de ces concordances (soit 63,64 %) se sont révélées incorrectes et seulement huit (soit 36,36) correctes. » [17]

## Une puissance de calcul aveugle, porteuse de discriminations et d'arbitraire

Dans le contexte socio-idéologique contemporain, c'est le caractère discriminatoire des applications de l'intelligence artificielle qui est régulièrement souligné dans le débat public. Mais ne faut-il pas aller plus loin, et resituer ces discriminations frappantes dans une montée plus générale de l'*arbitraire technologique* ?

Qu'un certain nombre de dysfonctionnements algorithmiques soient rangés à l'enseigne de la discrimination (ethnique, sexuelle, etc.), cela s'entend car c'est une dimension récurrente et marquante de ces erreurs. L'intelligence artificielle est particulièrement porteuse de discriminations quand elle est utilisée pour rationaliser le tri des candidats à l'embauche et pour étayer le travail des polices. Les dispositifs de détection des traits de personnalité afin d'analyser « scientifiquement » les entretiens de recrutement ont des chances importantes de pénaliser, plus encore qu'auparavant, les candidats en situation de handicap, ou même ceux dont la personnalité et les façons de s'exprimer ne sont pas « dans la norme ».

> « Si les caractéristiques de leurs visages ou leurs manières de se tenir et/ou de s'exprimer diffèrent de […] l'écrasante majorité des données sur lesquelles les algorithmes de recrutement ont été entraînés pour assigner des scores, ces personnes risquent de ne pas voir leurs aptitudes à exercer un poste reconnues, même si leurs traits de personnalité seraient tout aussi bénéfiques à l'exercice de ce poste que ceux d'une personne dite valide. Comme le soulignait Laurence Devillers, professeure en intelligence artificielle à la Sorbonne, "il y a une

[17] *Ibid.*, p. 11.

dimension culturelle énorme dans notre façon de nous exprimer. Que fait-on des personnes bègues, de celles qui s'expriment naturellement lentement, de celles qui ont un accent ?". Par ailleurs, ces systèmes peuvent être directement discriminants en détectant notamment des faiblesses psychologiques ou des problèmes mentaux qui relèvent des critères de discrimination de l'état de santé. » [18]

En ce qui concerne l'usage des algorithmes par les forces de l'ordre, le travail de la sociologue américaine Sarah Brayne montre combien ces outils sont susceptibles d'aggraver les biais préexistants des pratiques policières. Son enquête sur la police de Los Angeles [19] illustre comment l'usage des logiciels de Palantir provoque une mise sous surveillance accrue des quartiers pauvres, noirs et latinos, tout en conférant une impression d'objectivité aux choix effectués par les agents et leurs supérieurs. Le système à points de l'entreprise de Peter Thiel est censé justement neutraliser les préjugés légalement contestables des agents de police ; mais il renferme des biais qui créent un cercle vicieux – en fait, qui renforcent le cercle vicieux déjà en place dans les pratiques de répression classiques (délinquance – arrestations – incarcérations – plus de délinquance, etc.) : les personnes présentant des scores élevés dans les bases de données font l'objet d'une surveillance accrue, elles ont donc plus de chances d'être arrêtées et de récolter ainsi des points en plus.

De façon générale, il semble que les systèmes « intelligents » d'authentification et d'identification se trompent le plus fréquemment à propos des femmes, des enfants, des personnes transgenre et à la peau foncée. Le problème viendrait à la fois du manque de représentativité des données mobilisées lors de la phase d'apprentissage des algorithmes, et de la traduction mathématique de pratiques et comportements discriminatoires existants dans la société. Évidemment, à considérer ces biais, on peut (dans une certaine mesure) s'attendre à ce qu'ils soient progressivement gommés et corrigés. Mais mon propos n'est pas ici d'en appeler à une intelligence artificielle rigoureuse, fiable et non discriminante. Je terminerai plutôt en réinscrivant ces biais discriminatoires choquants dans une tendance plus large à la banalisation de l'arbitraire par ce type de technologie.

En effet, les algorithmes d'intelligence artificielle sont porteurs d'injustices qui vont au-delà de la discrimination de groupes particuliers ou minoritaires.

---

[18] Claire Hédon, *Rapport – Technologies biométriques, op. cit.*, p. 13.

[19] Sarah Brayne, « Big Date Surveillance : The Case of Policing », *American Sociological Review*, vol. 82, n°5, 2017.

Qu'on pense à celui employé par la Caisse d'allocations familiales (Caf), en France, qui « mouline » une quarantaine de paramètres issus de la surveillance électronique quotidienne pour attribuer une note (un « score de suspicion ») à ses millions d'allocataires. Le travail d'enquête mené par les collectifs Stop Contrôles et Changer de cap, avec l'association La Quadrature du Net, met en évidence que l'algorithme de la CAF cible les personnes les plus précaires : celles dont les revenus sont faibles ou irréguliers ; celles qui sont au chômage ; celles qui sont au RSA ; celles qui habitent un quartier « défavorisé » ; celles qui consacrent une part importante de leurs revenus à leur loyer ; celles qui bénéficient de l'Allocation Adulte Handicapé (AAH) ; celles qui élèvent des enfants seules (familles monoparentales).

La Quadrature du Net qualifie cet algorithme de discriminatoire, ce qui est à la fois vrai mais réducteur, dans la mesure où l'on voit bien que le nombre de citoyens français qui répondent à au moins un de ces critères est considérable – il dépasse certainement la dizaine de millions. Il s'agit d'un pan (de plus en plus) important de la population, que l'on peut qualifier de pauvre, de précaire, de surexploitée dans le travail, ou mise à l'écart de l'emploi et de la production. Dans son article de synthèse sur les méthodes de la Caf, la Quadrature souligne d'ailleurs que ce fameux algorithme a été conçu pour détecter les trop-perçus d'allocations, qui ont pour cause principale des erreurs déclaratives involontaires liées à la complexité des règles et des formulaires à remplir. Au fond : l'attribution bureaucratique des aides sociales est si complexe qu'elle recèle une part d'arbitraire ; et pour lutter contre les dysfonctionnements d'attribution, la bureaucratie met en place des dispositifs technologiques pour les identifier… dispositifs qui génèrent à leur tour de l'arbitraire. Bien sûr, un arbitraire qui pénalise plus ceux et celles qui sont déjà dans des situations fragiles, voire catastrophiques. Malgré sa mauvaise foi et son aveuglement devant la guerre aux pauvres menées par son institution, il y a aussi quelque chose de juste dans la réponse faite par un directeur de Caf aux critiques adressées au système de notation des allocataires : « l'algorithme est neutre », il est « l'inverse d'une discrimination » puisque « nul ne peut expliquer pourquoi un dossier est ciblé » [20].

[20] Voir l'article de La Quadrature du Net, « Notation des allocataires : l'indécence des pratiques de la Caf désormais indéniable », 27 novembre 2023.

S'appuyant sur l'ouvrage au titre évocateur d'une politologue américaine (*Automating Inequality*, de Virginia Eubanks), Kate Crawford souligne que les systèmes d'intelligence artificielle déployés dans le cadre de l'État-providence servent globalement à surveiller et évaluer les gens modestes, pour limiter leur accès aux ressources publiques. Elle donne l'exemple de deux programmes d'austérité impulsés au début des années 2010 par un gouverneur républicain du Michigan issu de l'industrie informatique, Rick Snyder. Il demanda la mise en place d'un algorithme visant à exclure les « criminels en fuite » (c'est-à-dire des personnes sous le coup d'un mandat d'arrêt non exécuté) de l'aide alimentaire : cet algorithme désigna à tort plus de 19 000 habitants du Michigan, automatiquement radiés de l'aide alimentaire !

> « Le second programme, baptisé Michigan Integrates Data Automated System (Midas), a été conçu pour juger "robotiquement" et punir ceux qui, d'après [lui], fraudaient l'assurance chômage de l'État. Midas traitait presque toutes les divergences ou incohérences dans les données d'une personne comme une preuve de comportement illégal. Le système identifia à tort plus de 40 000 habitants du Michigan. Les conséquences furent graves : saisie de remboursements d'impôt, saisie-arrêt des salaires, pénalités administratives dont le montant était quatre fois supérieur aux sommes concernées par les fraudes prétendues. En fin de compte, les deux systèmes furent de gigantesques échecs financiers, qui coûtèrent au Michigan bien plus qu'ils ne lui rapportèrent. Les victimes ont pu poursuivre l'État, mais seulement après que des milliers de personnes ont été touchées, avec de nombreux cas de faillites. » [21]

Il y a là quelque chose de décisif : des entrepreneurs, des politiciens, des journalistes, peuvent continuer de propager la foi dans la rationalité et l'efficacité de ces technologies, alors qu'elles sont responsables de tels méfaits, et porteuses d'un arbitraire radical. De même que l'intelligence artificielle peut programmer et entraîner, par ses calculs, la mort de dizaines de personnes sans lien avec les guerriers visés par une frappe militaire [22], elle peut provoquer des radiations et des désastres matériels sans retour dans la vie de milliers de familles. Mais quels que soient les erreurs et les dégâts, elle ne se voit jamais privée de son auréole de rationalité.

---

[21] Kate Crawford, *op. cit.*, p. 239.

[22] Voir Laure de Roucy-Rochegonde, Amélie Ferey, « Bombardements israëliens à Gaza : comment l'intelligence artificielle annihile les préventions éthiques », *Mediapart*, 7 mai 2024.

Dans son maître-ouvrage sur le sujet, Hannah Arendt mentionne le règne de l'arbitraire comme un des caractères essentiels du totalitarisme [23]. Si l'informatisation du monde et la surveillance « intelligente » nous amènent à une situation totalitaire, c'est peut-être surtout du fait de l'arbitraire que peut générer, sans protestation d'ampleur, l'usage systématique des machines computationnelles. Sans protestation d'ampleur, car domine jusqu'ici dans la société contemporaine une foi profonde dans la rationalité de ces machines. Quand Laurent Wauquiez (parmi d'autres) réclame de toute urgence l'instauration de la reconnaissance faciale dans les établissements scolaires, après un attentat islamiste dans un collège, il s'attaque frontalement à l'héritage européen de libertés civiles, dans la mesure où celui-ci s'est construit autour de la nécessité morale et politique de protéger les individus contre l'arbitraire des souverains. Il n'affirme pas simplement que la sécurité est plus importante que la liberté ; dans un moment d'effroi, il fait avancer dans les esprits l'idée que la technologie et sa puissance de calcul sont pleinement fiables – qu'elles sont en fait le véritable souverain de notre époque, qui seul permettra de maîtriser le chaos du monde.

C'est cette affirmation – ce bluff technologique – qu'il faut combattre, et partager au contraire la conviction que l'intelligence artificielle ne fait que renforcer le chaos : elle mine partout la stabilité du monde, dont la vie humaine a besoin pour s'abriter et se développer.

Matthieu Amiech.

Article publié dans la revue *Écologie & Politique* n°65,
"**L'ombre de l'IA**, ravages, déshumanisation et servitude",
éd. Le Bord de l'eau, novembre 2024.

[23] Hannah Arendt, *Les Origines du totalitarisme*, Paris, Gallimard, 2002.

Mon article vise à nous demander ce qu'il y a précisément de nouveau dans ces nouveautés, et où se situent les éventuels basculements.

Je resituerai les évolutions les plus récentes dans le processus d'informatisation des sociétés de ces trente dernières années, qui détermine largement, au-delà de telle ou telle application particulière, le recul considérable des possibilités d'anonymat et de vie privée.

Je me pencherai ensuite sur les conséquences des étapes actuelles du déferlement technologique en matière de libertés civiles, en mettant en avant la montée de l'arbitraire bureaucratique à mesure que s'étend le champ d'application de la soi-disant intelligence artificielle.

**Prix Libre**